UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/683,919	03/01/2002	Larry Lawson Jones	076706-201701/US	3793

73319   7590   12/09/2008
Greenberg Traurig, LLP (OnSpec/TPL)
2450 Colorado Avenue
Suite 400E
Santa Monica, CA 90404

EXAMINER
ZIA, SYED

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	09/683,919	JONES ET AL.
	Examiner	Art Unit	
	SYED ZIA	2431	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>24 September 2008</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-3, 10-14, 21, 23 and 24</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-3, 10-14, 21, 23 and 24</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail. Date _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on September 24, 2008 has been entered.

Response to Amendment

        This office action is in response to request for continuing examination and amendments

filed on September 24, 2008. Original application contained Claims 1-21. Applicant previously

amended Claims 1-5, 7, 9, 11-16, and 18, added new Claims 22-23, and cancelled Claims 4-5,

15-16, 23. Applicant currently amended Claim 11 and added a new Claim 24. The amendment

filed have been entered and made of record. Therefore, presently pending claims are 1-3, 10-14,

21 and 23-24.

Response to Arguments

        Applicant's arguments filed on September 24, 2008 have been fully considered but they

are not persuasive because of the following reasons:

Applicants argued regarding independent Claims 1, and 11 and stated that the cited prior

Abbott and Burger fail to teach or suggest storage unique "*identifiers of locations the apparatus*

and the individual have visited" and further stated that "*When Burger does discuss a "list of*

currently authorized locations for interface stations 104" (par. 0146), Burger describes that this

list is stored in database 406 of the network server 114 (par. 0146, Figs. 1 and 4). Storage on the

network server is not the same as storage on the pocket vault. Further, Burger makes clear that

the network server 114 is used to "track activity of Pocket Vault holders" (par. 0111). Thus,

Burger describes that the tracked activity of a user, including transactions, will be stored on

network server 114, and not the pocket vault".

This is not found persuasive. Application argument as best understood reading the

minimal and cryptic description of "storing unique Id of location" in the disclosure (paragraph

0016, 0021, and 0023], it was found that applicant claimed storage device, when used in the

exemplary network environment [Fig.4-5 paragraph 22-23], interfaces with a personal computer

at the key touchpoint. The personal computer at the <u>touchpoint accesses the **secure (central) key**</u>

<u>**hub** in order to acquire information and then to match that information with information received</u>

<u>from the secure key device.</u> Accordingly, the information would be obtained by accessing the

individual ID, accessing the device ID, then reading the log of the device and logging the

touchpoint information within the device [paragraph 0022]. Therefore, applicant claimed storage

device only keep identifier (a database key or ID provided by secure central key hub) of the

locations visited. Cited prior art Burger discloses a list of currently authorized locations for

interface stations 104 stored in database 406 of the network server 114 (paragraph. 0146, Figs. 1

and 4) where the Packet Vault can be used by sending interface unit identifier (a database key or

ID) to the network server. Thus, cited prior art does teach accessing authorized location by

sending an identifier to a central server.

As a result, the system of cited prior art(s) does implement and teaches a system and

method that relates to providing a device for secure identification which also make use of

presently available installed infrastructure.

Applicants <u>clearly</u> have failed to explicitly identify specific claim limitations, which

would define a patentable distinction over prior arts.

Therefore, the examiner asserts that the system of cited prior arts does teach or suggest

the subject matter broadly recited in independent Claims and in subsequent dependent Claims.

Accordingly, rejections for claims 1-3, 10-14, 21 and 23-24 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 10-14, 21 and 23-24 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Abbott et al. (U. S. Patent 6,671,808), and further in view of Burger (U. S.

Pub. 2005/0060586 A1) (hereafter Burger).

1.   Regarding Claim 1 Abbott teach and describe an apparatus (Fig.2, and 4) comprising: a

port; a storage medium coupled to a and accessed by controller, wherein, the storage medium is

to store an encrypted unique identifier of the apparatus, encrypted identity information of an

individual pre-associated with the apparatus and an encrypted log of unique identifier of

locations the apparatus and the individual have visited, the controller coupled to the port to

record in the encrypted log on the storage medium, a unique identifier corresponding to a

locations the apparatus and the individual have visited; the controller configured to restrict the

individual from modifying the encrypted unique identifier of the apparatus, encrypted identity

information of the individual pre-selected with the apparatus, encrypted log of unique identifiers

of locations the apparatus and the individual have visited as stored in the storage medium; and

the controller, configured to provide, in response to a request from an authorized requestor, one

or more of the unique identifier of the apparatus, identity information of the individual pre-

associated with the apparatus, and the unique identifiers of locations the apparatus and the

individual have visited (col.3 line 26 to col.4 line 7, col.4 line 50 to line 62, col.5 line 12 to line

15, col.5 line 55 to col.6 line 60, and col.7 line 38 to col.9 line 65).

        Although the system disclosed by Abbot shows all the features of the claimed limitation,

as well as secure identification of individuals (users) when using the unique USB enabled device

but Abbot does not specifically discuss in detail unique identifier of the apparatus, encrypted

identity information of an individual pre-associated with the apparatus, and the identity of

locations of network nodes to which apparatus communicated with during transactions.

        In an analogous art, Burger, on the other hand discloses computing environment that

 describe methods of portable electronic authorization system (Fig.1-2, 4) by engaging

transactions involving financial and/or non-financial media and devices, where apparatus has an

authenticator that authenticates an identity of a user, and interface station conducting

registration process when device access different locations [Fig.1-2, and paragraph 0019 –

0020, 0114 -0118, and 0146].

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Abbot and Burger, because Burger's system of portable

electronic authorization with plurality of unique devices for providing plurality of services, such

as device management, business transaction, and location management, after authenticating the

device and user by using embedded ID would not only enhance the trustworthiness of the user

of portable device when tracking the device in a external network but will also generate a log of

transactions and location where device was communicated and used   (co.7 line 9 to line 15).

2.   Regarding Claim 11 Abbott teach and describe a system for allowing for secure

identification of an individual when accessing information (Fig.2, and 4) comprising: a central

hub configured to communicate with a plurality of touchpoints, at least one of the plurality of

touchpoints configured to communicate with at least one device; the at least one device

comprising a port; a storage medium coupled to and accessed by a controller, wherein the storage

medium is configured to store an encrypted unique identifier of the apparatus, encrypted identity

information of an individual pre-associated with the apparatus, and an encrypted log of unique

identifiers of locations the apparatus and the individual have visited; the controller, coupled to

the port, configured to record in the encrypted log on the storage medium, a unique identifier

corresponding to a location the apparatus and the individual have visited; the controller

configured to restrict the individual from modifying the encrypted unique identifier of the

apparatus, encrypted identity information of the individual pre-associated with the apparatus, and

the encrypted log of unique identifiers of locations the apparatus and the individual have visited,

as stored in the storage medium; and

the controller, configured to provide, in response to a request from an authorized requestor, one

or more of the unique identifier of the apparatus, identity information of the individual pre-

associated with the apparatus, and the log of unique identifiers of locations the apparatus and the

individual have visited (col.3 line 26 to col.4 line 7, col.4 line 50 to line 62, col.5 line 12 to line

15, col.5 line 55 to col.6 line 60, and col.7 line 38 to col.9 line 65).

Although the system disclosed by Abbot shows all the features of the claimed limitation,

as well as secure identification of individuals (users) when using the unique USB enabled device

but Abbot does not specifically discuss in detail unique identifier of the apparatus, encrypted

identity information of an individual pre-associated with the apparatus, and the identity of

locations of network nodes to which apparatus communicated with during transactions.

In an analogous art, Burger, on the other hand discloses computing environment that

describe methods of portable electronic authorization system (Fig.1-2, 4) by engaging

transactions involving financial and/or non-financial media and devices, where apparatus has an

authenticator that authenticates an identity of a user, and interface station conducting

registration process when device access different locations [Fig.1-2, and paragraph 0019 –

0020, 0114 -0118, and 0146].

Therefore, It would have been obvious to one ordinary skilled in the art at the time of

invention to combine the teachings of Abbot and Burger, because Burger's system of portable

electronic authorization with plurality of unique devices for providing plurality of services, such

as device management, business transaction, and location management, after authenticating the

device and user by using embedded ID would not only enhance the trustworthiness of the user

of portable device when tracking the device in a external network but will also generate a log of

transactions and location where device was communicated and used (co.7 line 9 to line 15).

3.   Regarding Claim 24 Abbott teach and describe a secure key hub to serve as a centralized

data collection point, the hub configured to:

receive and store information from at least one touchpoint regarding usage of a secure key device

at the at least one touchpoint, the secure key device comprising a storage medium configured to

store an encrypted unique identifier of the secure key device, encrypted identity information of a

user of the secure key device, and an encrypted log of identifiers of locations at which the secure

key device has been used; and provide information to the at least one touchpoint to match with

information received by the at least one touchpoint from the secure key device in order to

identify the user of the secure key device (col.3 line 26 to col.4 line 7, col.4 line 50 to line 62,

col.5 line 12 to line 15, col.5 line 55 to col.6 line 60, and col.7 line 38 to col.9 line 65).

        Although the system disclosed by Abbot shows all the features of the claimed limitation,

as well as secure identification of individuals (users) when using the unique USB enabled device

but Abbot does not specifically discuss in detail unique identifier of the apparatus, encrypted

identity information of an individual pre-associated with the apparatus, and the identity of

locations of network nodes to which apparatus communicated with during transactions.

In an analogous art, Burger, on the other hand discloses computing environment that describe methods of portable electronic authorization system (Fig.1-2, 4) by engaging transactions involving financial and/or non-financial media and devices, where apparatus has an authenticator that authenticates an identity of a user, and interface station conducting registration process when device access different locations [Fig.1-2, and paragraph 0019 – 0020, 0114 -0118, and 0146].

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Abbot and Burger, because Burger's system of portable electronic authorization with plurality of unique devices for providing plurality of services, such as device management, business transaction, and location management, after authenticating the device and user by using embedded ID would not only enhance the trustworthiness of the user of portable device when tracking the device in a external network but will also generate a log of transactions and location where device was communicated and used   (co.7 line 9 to line 15).

4.   Claims 2-3, 10, 12-14, and 21, and 23 are rejected applied as above rejecting Claims 1, and 11. Furthermore, the system of Abbott and Burger teaches and describes a system   wherein

As per Claim 2, the port comprises any one of a firewire port, USB port or an infiniband port (Abbot: col.3 line 26 to line 30, col.5 line 12 to line 14, Fig.1, Item 130, Fig.4 Item 402))

As per Claim 3, the storage medium comprises a memory (Abbot: Fig. 2A, col.4 line 50 to line 62).

As per Claim 10, the security information can be enhanced or modified by downloading data to the apparatus (Abbot: col.8 line 20 to line 33 and col.10 line 6 to line 11).

As per Claim 12, the port comprises any one of a firewire port, USB port or an infiniband port (Abbot: col.3 line 26 to line 30, col.5 line 12 to line 14, Fig.1, Item 130, Fig.4 Item 402).

As per Claim 13, at least one of the plurality of touchpoints comprises a personal computer (Abbot: Fig.1 Item 102).

As per Claim 14, the storage medium comprises a flash memory (Abbot: Fig. 2A, col.4 line 50 to line 62).

As per Claim 21, the security information within the at least one device can be enhanced or modified by downloading data to the at least one device (Abbot: col.8 line 20 to line 33, and col.10 line 6 to line 11).

As per Claim 23, the touchpoints comprises any one of airports, car rentals, or banks (Burger: [0125, 0135, and 0152]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
December 4, 2008
/Syed   Zia/
Primary Examiner, Art Unit 2431